❒ Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
information about the location of the cellular telephone assigned IP Address 2607:fb90:9a01:4e0d:0000:0005:b295:6b01, which was used at multiple times listed in Attachment A between April 21, 2021 and April 25, 2021 (the "Target Cell Phone")

Case No. 21-M-386 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See attachment B

YOU ARE COMMANDED to execute this warrant on or before 5-27-21 *(not to exceed 14 days)*

❒ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries.
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☑ for 30 days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 5-13-21. 2:45 pm

Stephen C. Dries
Judge's signature

City and state: Milwaukee, WI.

Honorable Stephen C. Dries
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

1. Records and information associated with the cellular device assigned IP Address 2607:fb90:9a01:4e0d:0000:0005:b295:6b01, utilized at the following dates and times:

- Time 2021-04-21 03:15:08 UTC
- Time 2021-04-21 03:16:12 UTC
- Time 2021-04-21 03:16:15 UTC
- Time 2021-04-21 04:51:44 UTC
- Time 2021-04-21 12:27:55 UTC
- Time 2021-04-21 12:39:19 UTC
- Time 2021-04-21 13:46:58 UTC
- Time 2021-04-21 19:38:21 UTC
- Time 2021-04-21 19:38:21 UTC
- Time 2021-04-22 02:25:56 UTC
- Time 2021-04-22 22:45:18 UTC
- Time 2021-04-22 23:41:15 UTC
- Time 2021-04-23 03:44:02 UTC
- Time 2021-04-23 03:48:43 UTC
- Time 2021-04-23 03:48:46 UTC
- Time 2021-04-23 19:18:54 UTC
- Time 2021-04-23 19:19:08 UTC
- Time 2021-04-23 19:19:35 UTC
- Time 2021-04-24 04:35:45 UTC
- Time 2021-04-24 09:27:58 UTC
- Time 2021-04-25 23:38:12 UTC
- Time 2021-04-25 23:38:12 UTC

(referred to herein and in Attachment B as "the Target Cell Phone"), that is in the custody or control of T-Mobile (referred to herein and in Attachment B as the "Service Provider"), a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054.

2. The Target Cell Phone.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period of March 29, 2021 to May 13, 2021:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address);

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(ii) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received).

b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication.

The Court has also issued an order pursuant to 18 U.S.C. § 3123, for such information associated with the Target Cell Phone.

c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. "Information about the location of the Target Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the

Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 18, United States Code, Section 1073 (flight to avoid prosecution) and Wisconsin Statute 940.01(1)(a) (first-degree intentional homicide), involving Santos M. SOLIER since March 30, 2021.

All information described above in Section I that will assist in arresting Santos M. SOLIER, who was charged with violating Title 18, United States Code, Section 1073 (flight to avoid prosecution) and Wisconsin Statute 940.01(1)(a) (first-degree intentional homicide), is the subject of an arrest warrant issued on April 8, 2021, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information about the location of the cellular telephone assigned IP Address 2607:fb90:9a01:4e0d:0000:0005:b295:6b01, which was used at multiple times listed in Attachment A between April 21, 2021 and April 25, 2021 (the "Target Cell Phone")

Case No. 21-M-386 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Wis. Stat. § 940.01(1)(a) and Wis. Stat. § 939.05	See attached affidavit

The application is based on these facts:

See attached affidavit

- ☐ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Bryon Downey
Digitally signed by Bryon Downey
Date: 2021.05.13 14:28:41 -05'00'

Applicant's signature

USMS TFO Bryon Downey

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone/email *(specify reliable electronic means)*.

Date: 5-13-21

Stephen C. Dries

Judge's signature

City and state: Milwaukee, WI.

Honorable Stephen C. Dries

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Police Officer Bryon Downey, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A), for information about the location of the cellular telephone assigned IP Address 2607:fb90:9a01:4e0d:0000:0005:b295:6b01, which was used at multiple times listed in Attachment A between April 21, 2021 and April 25, 2021 (the "Target Cell Phone"), whose service provider is T-Mobile ("Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054. The Target Cell Phone is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the Target Cell Phone.

3. On May 11, 2021, the United States submitted applications for a warrant for location information about and seeking authorization to install and use pen registers and trap and trace devices for the Target Cell Phone. The Court issued the order and warrant in Application No. 14190 and Case No. 21-M-377 (SCD). Upon execution of that warrant, T-Mobile was unable to identify the Target Cell Phone based on the single IP address login listed on that warrant. The United States seeks now to provide T-Mobile multiple IP logins for the same IP

address, so that T-Mobile can properly identify the Target Cell Phone.

4. I am a Task Force Officer with the United States Marshals Service, and I have been employed full time as a Police Officer with the Milwaukee Police Department for over 17 years. One of my primary duties is to investigate and arrest state and federal fugitives. I have obtained my Wisconsin Law Enforcement Certification through the Milwaukee Police Department Training Academy in Milwaukee, Wisconsin. I have been assigned to the United States Marshals Service's Fugitive Task Force since December 2019, and I have been involved in numerous fugitive investigations during this period. Many of these investigations were aided by records related to electronic communications and the subsequent analysis of those records. In most of those cases, the records provided critical investigative leads and corroborating evidence. I have had previous experiences using electronic location data in order to locate and apprehend fugitives from justice. I am an investigator or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, in that I am empowered by law to conduct investigations of and arrests for federal offenses.

5. The facts in this affidavit come from my training, experience, and information and documents provided to me by other law enforcement officers. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that Santos M. SOLIER has violated Title 18, United States Code, Section 1073 (flight to avoid prosecution) and Wisconsin Statute 940.01(1)(a) (first-degree intentional homicide). There is also probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and will assist law enforcement in arresting SOLIER, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

JURISDICTION

7. The Court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. On March 30, 2021, the State of Wisconsin issued a criminal complaint charging SOLIER with first-degree intentional homicide, in violation of Wisconsin Statute 940.01(1)(a) (first-degree intentional homicide) in Milwaukee County Case No. 2021CF001209. An arrest warrant (Milwaukee Police Department Warrant No. K01453) was issued with authorization for nationwide extradition that same day.

9. On April 8, 2021, this Court issued an arrest warrant for SOLIER based upon a violation of Title 18, United States Code, Section 1073 (flight to avoid prosecution) in Case No. 21-MJ-081. SOLIER remains a fugitive from justice. The United States Marshals Service is leading the investigation to locate and arrest SOLIER.

10. Since the issuance of the arrest warrant, the Milwaukee Police Department Fugitive Apprehension Unit and the United States Marshals Service has made multiple attempts to apprehend SOLIER, but SOLIER was able to flee the state in attempt to avoid prosecution.

11. On April 7, 2021, I conducted an open-source search and found SOLIER's Facebook profile under https://www.facebook.com/josh.rackedup, Facebook User ID 100015783785535, with a user name of "Josh Rackedup."

12. I observed multiple posts on this Facebook profile between April 20, 2021 and April 26, 2021, butalso know that not all Facebook content is visible to the public. I was able to identify this Facebook profile as SOLIER's by comparing Department of Transportation and booking photographs to these depicted in the publicly displayed photos

within the Facebook account.

13. On April 12, 2021, the Honorable William E. Duffin authorized the installation and use of pen registers and trap and trace devices, as well as a search warrant for content related to SOLIER's Facebook account—https://www.facebook.com/josh.rackedup, Facebook User ID 100015783785535.

14. On April 24, 2021, I conducted another open-source search and observed that SOLIER changed his Facebook screen name to "Hen Er Ton," using the same Facebook User ID 100015783785535.

15. The results of the ongoing pen-trap device on SOLIER's Facebook account shows that between the dates of April 21, 2021 and April 25, 2021, SOLIER has logged in to his Facebook account using the IP address 2607:fb90:9a01:4e0d:0000:0005:b295:6b01—multiple date and login times are listed in Attachment A—the Target Cell Phone. These records have shown that SOLIER is actively using his Facebook account, using a device serviced by T-Mobile.

16. I know that subjects who are wanted for crimes and are trying to flee frequently use social media to communicate with family, friends, and accomplices. It is common for wanted subjects to set these social media accounts to "private" or lock the access tothem, use aliases, and use accounts of other persons to avoid law enforcement detection.

TECHNICAL BACKGROUND: DYNAMIC IP ADDRESSES

17. I used the website www.arin.net, the American Registry of Internet Numbers (ARIN), to obtain the owner and operator of the IP address for the Target Cell Phone. According to ARIN, the listed IP address is serviced by **T-Mobile**. I have utilized ARIN in the past and know this website to be reliable.

18. Based on training, experience and information provided to me by other law enforcement officers, I know that **T-Mobile** is a cellular service provider that has the ability

to connect a cellular service to the internet through Dynamic Internet Protocols. A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it is connected to a network. A dynamic IP address is an automatically configured IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server to every new network node.

19. Dynamic IP addresses are generally implemented by Internet service providers and networks that have a large number of connecting clients or end-nodes. Unlike static IP addresses, dynamic IP addresses are not permanent. A dynamic IP is assigned to a node until the device is connected to the network; therefore, the same node may have a different IP address every time the device reconnects with the network.

20. I know through training, experience and information provided to me by other law enforcement officers that **T-Mobile** is able to "resolve" associated Dynamic IP addresses. When **T-Mobile** "resolves" those IP addresses, they are able to identify the associated user and the specific cellular phone associated with that user. In other words, when **T-Mobile** is providedwith a particular associated IP address and time stamp (like the IP address and time stamps described here and listed in Attachment A), **T-Mobile** is able to (i) determine the particular cellular phone that utilized that IP address; and (ii) collect cell-site location data associated with that same particular cellular phone, in the manner described below.

TECHNICAL BACKGROUND: CELL SITE LOCATION DATA

21. In my training, experience and information provided to me by other law enforcement officers, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector

records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half- mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

22. Based on my training, experience, and information provided to me by other law enforcement officers, I know that the Service Provider can collect cell-site data on a prospective basis about the Target Cell Phone. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

23. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular

telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas.

24. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data. Based on my training, experience, and information provided to me by other law enforcement officers, I know that the Service Provider can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available.

25. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

26. Based on my training, experience and information provided to me by other law enforcement officers, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider

typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training, experience and information provided to me by other law enforcement officers, this information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

27. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

28. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

29. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

30. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result,

as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cell Phone would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

31. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.

ATTACHMENT A

Property to Be Searched

1. Records and information associated with the cellular device assigned IP Address 2607:fb90:9a01:4e0d:0000:0005:b295:6b01, utilized at the following dates and times:

- Time 2021-04-21 03:15:08 UTC
- Time 2021-04-21 03:16:12 UTC
- Time 2021-04-21 03:16:15 UTC
- Time 2021-04-21 04:51:44 UTC
- Time 2021-04-21 12:27:55 UTC
- Time 2021-04-21 12:39:19 UTC
- Time 2021-04-21 13:46:58 UTC
- Time 2021-04-21 19:38:21 UTC
- Time 2021-04-21 19:38:21 UTC
- Time 2021-04-22 02:25:56 UTC
- Time 2021-04-22 22:45:18 UTC
- Time 2021-04-22 23:41:15 UTC
- Time 2021-04-23 03:44:02 UTC
- Time 2021-04-23 03:48:43 UTC
- Time 2021-04-23 03:48:46 UTC
- Time 2021-04-23 19:18:54 UTC
- Time 2021-04-23 19:19:08 UTC
- Time 2021-04-23 19:19:35 UTC
- Time 2021-04-24 04:35:45 UTC
- Time 2021-04-24 09:27:58 UTC
- Time 2021-04-25 23:38:12 UTC
- Time 2021-04-25 23:38:12 UTC

(referred to herein and in Attachment B as "the Target Cell Phone"), that is in the custody or control of T-Mobile (referred to herein and in Attachment B as the "Service Provider"), a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, New Jersey 07054.

2. The Target Cell Phone.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period of March 29, 2021 to May 13, 2021:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address);

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(ii) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received).

b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication.

The Court has also issued an order pursuant to 18 U.S.C. § 3123, for such information associated with the Target Cell Phone.

c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. "Information about the location of the Target Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the

Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence and instrumentalities of violations of Title 18, United States Code, Section 1073 (flight to avoid prosecution) and Wisconsin Statute 940.01(1)(a) (first-degree intentional homicide), involving Santos M. SOLIER since March 30, 2021.

All information described above in Section I that will assist in arresting Santos M. SOLIER, who was charged with violating Title 18, United States Code, Section 1073 (flight to avoid prosecution) and Wisconsin Statute 940.01(1)(a) (first-degree intentional homicide), is the subject of an arrest warrant issued on April 8, 2021, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.